

İÇİNDEKİLER

SUNUŞ	5
İÇİNDEKİLER	7
TABLOLAR LİSTESİ	13
ŞEKİLLER LİSTESİ	15
KISALTMALAR	17
GİRİŞ	19

BİRİNCİ BÖLÜM

KURUMSAL

SİBER GÜVENLİK YÖNETİMİNİN ÖNEMİ	27
1.1. GENEL OLARAK	27
1.2. SİBER TEHDİTLERLE MÜCADELE YÖNTEMLERİ	32
1.2.1. Teknolojik Yöntem ve Araçlarla Mücadele	35
1.2.1.1. Donanım Güvenliği	36
1.2.1.2. Yazılım Güvenliği	37
1.2.1.3. Ağ Güvenliği	38
1.2.2. Teknoloji Dışı Yöntem ve Araçlarla Mücadele	39
1.2.2.1. Kurumsal Siber Güvenlik Kural ve Yönergeleri	41
1.2.2.2. Prosedür ve Kontrol Bileşenleri	43
1.2.2.3. Mücadele Araç ve Metotları	43
1.2.2.4. Farkındalık Çalışmaları	44
1.3. SİBER GÜVENLİKTE ON ADIM KURALI	45
1.3.1. Birinci Adım: Siber Güvenlik Risk Yönetim Sisteminin Belirlenmesi	47
1.3.2. İkinci Adım: Güvenli Yapılandırma	47
1.3.3. Üçüncü Adım: Ağ Güvenliği	48
1.3.4. Dördüncü Adım: Kullanıcı Yetki Yönetimi	48
1.3.5. Beşinci Adım: Kullanıcı Eğitimi ve Farkındalık	49
1.3.6. Altıncı Adım: Olay Yönetimi	49
1.3.7. Yedinci Adım: Kötü Niyetli Yazılımlardan Korunma	50
1.3.8. Sekizinci Adım: İzleme	50

1.3.9. Dokuzuncu Adım: Taşınabilir Depolama Aygıtlarının Kontrolleri	51
1.3.10. Onuncu Adım: Evden veya Mobil Çalışma.....	51
1.4. SİBER GÜVENLİK ÖNLEMLERİNİN MUKAYESESİ	51
1.4.1. ISM Benchmark Analiz Sonuçları.....	53
1.4.1.1. Serpilme Diyagramı.....	53
1.4.1.2. Radar Grafikleri	54
1.4.2. ISM Benchmark Kullanılarak Yapılan Araştırmalar	56

İKİNCİ BÖLÜM

KURUMSAL SİBER GÜVENLİK YÖNETİMİNİN KAVRAMSAL ÇERÇEVESİ

2.1. BİLGİ VE İLETİŞİM TEKNOLOJİLERİ.....	59
2.1.1. Siber Güvenlik Bağlamında BİT'in Tarihçesi.....	60
2.1.2. İşletmeler İçin Bilişim ve İletişim Teknolojilerinin Önemi.....	66
2.2. BİLGİ GÜVENLİĞİ.....	68
2.3. SİBER GÜVENLİK	74
2.3.1. Siber Güvenliğin Temel Kavramları	75
2.3.1.1. Siber Varlık.....	75
2.3.1.2. Siber Olay.....	76
2.3.1.3. Siber Uzay	77
2.3.1.4. Siber Zorbalık	78
2.3.1.5. Siber Savaş	78
2.3.1.6. Siber Casusluk	79
2.3.1.7. Siber Silah	79
2.3.1.8. Siber Terörizm	80
2.3.1.9. Siber Saldırı ve Aşamaları.....	81
2.3.1.9.1. Birinci Aşama: Keşif ve Tanıma	82
2.3.1.9.2. İkinci Aşama: Tarama	83
2.3.1.9.3. Üçüncü Aşama: Erişim Sağlama	83
2.3.1.9.4. Dördüncü Aşama: Erişimi Sürdürme.....	84
2.3.1.9.5. Beşinci Aşama: İzleri Saklama.....	84
2.3.1.9.6. Engelleme Saldırıları.....	84
2.3.1.10. Siber Tehdit.....	86
2.3.2. Siber Tehdit Yöntem ve Çeşitleri.....	87
2.3.2.1. Kötü Amaçlı Yazılımlar (Malware)	89

2.3.2.1.1.	Bilgisayar Virüsleri.....	90
2.3.2.1.2.	Solucan ve Truva Atı	90
2.3.2.1.3.	Klavye İzleme (Key Logger) Yazılımları	91
2.3.2.1.4.	İstem Dışı Ticari Reklam ve Tanıtım (Adware) Yazılımları	91
2.3.2.1.5.	Bilgi Toplayan Casus/Köstebek (Spyware) Yazılımları	92
2.3.2.2.	Web-Tabanlı ve Web Uygulamalı Siber Saldırılar	92
2.3.2.3.	Botnet / Zombi Bilgisayar	94
2.3.2.4.	Hizmet Dışı Bırakma (Denial of Service – DOS).....	96
2.3.2.5.	Fiziksel Zarar / Hırsızlık / Kayıp	97
2.3.2.6.	İç Tehdit	98
2.3.2.7.	Oltalama.....	98
2.3.2.8.	İstenmeyen e-posta	99
2.3.2.9.	İstismar Kiti	99
2.3.2.10.	Veri İhlalleri	101
2.3.2.11.	Kimlik Hırsızlığı	103
2.3.2.12.	Bilgi Sızıntısı	104
2.3.2.13.	Fidye Yazılımları	104
2.3.2.14.	Siber Casusluk.....	105
2.3.2.15.	Gelişmiş Siber Tehdit.....	106
2.3.2.16.	Ağ Dinleme	107
2.3.2.17.	ARP Zehirlenmesi	108
2.3.2.18.	IP Aldatması.....	109
2.3.2.19.	Ortadaki Adam Saldırısı (Man in the Middle Attack)	109
2.3.2.20.	Kabloya Saplama Yapma	110
2.3.2.21.	Sosyal Mühendislik	111
2.3.3.	Siber Güvenlik Vakaları	112
2.3.3.1.	Estonya Vakası	112
2.3.3.2.	Gürcistan Saldırısı	113
2.3.3.3.	Kırgızistan Saldırıları.....	113
2.3.3.4.	Stuxnet Vakası.....	113
2.3.3.5.	Türkiye'ye Yapılan Saldırılar	113
2.4. SİBER GÜVENLİK STANDARTLARI.....		114
2.4.1.	Uluslararası Standartlar Teşkilatı ISO 27000 Standartlar Serisi.....	116

2.4.1.1.	ISO 27001	117
2.4.1.2.	ISO 27002	120
2.4.2.	Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri (COBIT)	121

ÜÇÜNCÜ BÖLÜM

KURUMSAL SİBER GÜVENLİK YÖNETİMİ ARAŞTIRMASI

3.1.	ARAŞTIRMANIN PROBLEM VE ALT PROBLEMLERİ	125
3.2.	ARAŞTIRMANIN AMACI.....	126
3.3.	ARAŞTIRMANIN ÖNEMİ	127
3.4.	ARAŞTIRMANIN HİPOTEZLERİ.....	128
3.5.	ARAŞTIRMANIN VARSAYIMLARI	132
3.6.	ARAŞTIRMANIN SINIRLILIKLARI	133
3.7.	ARAŞTIRMANIN YÖNTEMİ	133
3.8.	ARAŞTIRMANIN EVREN VE ÖRNEKLEMİ.....	134
3.9.	VERİ TOPLAMA ARAÇLARI.....	135
3.10.	PİLOT ÇALIŞMA	135
3.10.1.	Pilot Uygulama Keşfedici Faktör Analizi	138
3.10.2.	Pilot Uygulama Güvenilirlik Analizi	140
3.11.	FAKTÖR ANALİZLERİ.....	141
3.11.1.	Keşfedici Faktör Analizleri.....	141
3.11.1.1.	Siber Güvenliğine Kurumsal Yaklaşım Ölçeği KFA.....	142
3.11.1.2.	Fiziksel ve Çevresel Güvenlik Tedbirleri Ölçeği KFA	144
3.11.1.3.	Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri Ölçeği KFA	145
3.11.1.4.	Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri Ölçeği KFA	146
3.11.1.5.	Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi Ölçeği KFA.....	147
3.11.2.	Doğrulayıcı Faktör Analizleri	148
3.11.2.1.	Siber Güvenliğine Kurumsal Yaklaşım Ölçeği DFA.....	150
3.11.2.2.	Fiziksel ve Çevresel Güvenlik Tedbirleri Ölçeği DFA	152
3.11.2.3.	Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri Ölçeği DFA	152
3.11.2.4.	Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri Ölçeği DFA.....	153
3.11.2.5.	Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi Ölçeği DFA	154

3.12. GÜVENİLİRLİK ANALİZİ	156
3.13. NORMAL DAĞILIM TESTİ	157

DÖRDUNCÜ BÖLÜM
KURUMSAL SİBER GÜVENLİK ANALİZİ

4.1. DEMOGRAFİK BULGULAR.....	159
4.2. TANIMLAYICI İSTATİSTİKLER.....	165
4.3. T TESTİ	166
4.4. ANOVA (F) TESTİ.....	170
4.5. HİPOTEZ SONUÇLARI.....	182

SONUÇ VE ÖNERİLER

SONUÇLAR.....	187
ARAŞTIRMACILARA ÖNERİLER	195
İŞLETMELERE ÖNERİLER	196
KAYNAKÇA	199

EKLER

EK-1 UDHB KURUMLAR TARAFINDAN ALINMASI GEREKEN SİBER ÖNLEMLER	215
EK-2 ANKET SORULARI	219

KAYNAKÇA

- Aaker, D. A. (2007). *Strategic market management*. Hoboken, NJ: John Wiley & Sons.
- ABD Sağlık Hizmetleri. *Information memorandum*. U.S. Department Of Health And Human Services. <http://www.acf.hhs.gov/sites/default/files/cb/im1504.pdf> (Erişim Tarihi: 5 Ekim 2016)
- Acılar, A., *İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü,, Organizasyon ve Yönetim Bilimleri Dergisi*, Cilt 1, Sayı 1, 2009 sh.25-33.
- Aho, J., and Nevala, J., 2016. *Keskisuomalaisten yritysten kyberturvallisuus*. Jyväskylä. Principal Regional Council of Central Finland and Jyväskylän koulutuskuntayhtymä. http://edu360.fi/wp-content/uploads/2016/08/Yrityspuolen_kybertutkimus-FINAL-20160829.pdf (Erişim Tarihi: 15 Ekim 2016)
- Alagöz, A. ve Allahverdi, M., *Kurumsal Bilgi Güvenliği ve Muhasebe Bilgi Sistemi*, Muhasebe ve Vergi Uygulamaları Dergisi, 2011-3 sh.47-64.
- Albrechtsena, E., and Hovdena, J. (2009). *The information security digital divide between information security managers and users*. Computers & Security Volume 28, Issue 6, September 2009,, 28(6), 476–490.
- Alford, L. D. (2000). *Cyber warfare: protecting military systems*. The Journal of the Defense Acquisition University Review Quarterly, 7(2).
- Alter, S., and Sherer, S. (2004). *A general, but readily adaptable model of information system risk*. Communicaitons of the AIS, 14(1),1-28.
- Altunışık, R., Coşkun, R., Bayraktaroğlu, S. ve Yıldırım, E. (2010) *Sosyal bilimlerde araştırma yöntemleri*, SPSS Uygulamalı, 6. Baskı, Ankara, Pegem Akademi.
- Amerikan Savunma Bakanlığı. (2013). *Cyberspace operations*. DOD. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (Erişim Tarihi: 12 Kasım 2016)
- Anderson, R. (2001). *Why information security is hard—an economic perspective*. 17th Annual Computer Security Applications Conference. New Orleans: University of Cambridge Computer Laboratory.
- Arora, V. (2016). *Comparing different information security standards: COBIT v s. ISO 27001*. Carnegie Mellon University, Qatar., 7-9. <https://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf> (Erişim Tarihi: 12 Ekim 2016)

- ASD. (2016). *Strategies to Mitigate Targeted Cyber Intrusions*. Australian Signals Directorate:
http://www.asd.gov.au/publications/protect/Top_4_Mitigations.pdf (Erişim Tarihi: 25 Ekim 2016)
- Aspan, M. (2011). *Citi says 360,000 accounts hacked in May cyber-attack*. Reuters
<http://www.reuters.com/article/2011/06/16/us-citigroup-hacking-idUSTRE75F17620110616> (Erişim Tarihi: 18 Kasım 2016)
- Avnet. (2016). *Cyber attack how it works*.
<http://www.ts.avnet.com/uk/images/DDoS-Howitworks-4.jpg> (Erişim Tarihi: 3 Aralık 2016)
- Bakır, E. (2016). *5. Boyutta savaş: siber savaşlar - II*. Tubitak Bilgem:
<https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html> (Erişim Tarihi: 3 Eylül 2016)
- Bakır, E. (2011). *İnternet güvenliğinin tarihçesi*. TUBİTAK Bilgem Dergisi, 3(5), 16.
- Barrett, N. (2003). *Penetration testing and social engineering: Hacking the weakest link*. Information Security Technical Report, 8(4), 56-58
- Baskerville, R. (1993). Information systems security design methods: implications for information systems development. ACM Computing Surveys, 25, 375–414.
- Baykara, M., Daş, R. ve Karadoğan, İ., *Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi*, 1 st International Symposium on Digital Forensics and Security (ISDFS'13), 20-21 May 2013, sh.231-239 Elazığ, Turkey.
- Baykara, M., Daş, R., Karadoğan, İ., *Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi*, 1 st International Symposium on Digital Forensics and Security (ISDFS'13), 20-21 May 2013, sh.231-239 Elazığ, Turkey.
- Bayram, N. (2013), *Yapısal eşitlik modellemesine giriş*, Ezgi Kitabevi Yayınları, Ankara.
- Baze, A. (2016). Realistic risk management using the CIS 20 security controls. SANS Institute InfoSec Reading Room.
- Berghel, H. (2005). The two sides of RoI: return on investment vs. risk of incarceration. Communications of the ACM, 48(4), 15-20.
- BM Uluslararası Telekomünikasyon Birliği . (2008). X.1205 : Overview of cybersecurity. ITU. <https://www.itu.int/rec/T-REC-X.1205-200804-I> (Erişim Tarihi: 20 Ekim 2016)

- Borland, J. (2013). *For tor, publicity a mixed blessing*. Wired: <http://www.wired.com/2013/12/tor-publicity-mixed-blessing/>_(Erişim Tarihi: 10 Ekim 2016)
- Brandpowder. (2016). *How deep is your web*. Brandpowder <http://www.brandpowder.com/how-deep-is-your-web/>_(Erişim Tarihi: 28 Ekim 2016)
- Brown, G., and Poellet, K. (2012). *The customary international law of cyberspace*. Strategic studies, 127-145. <http://www.au.af.mil/au/ssq/2012/fall/brown-poellet.pdf>_(Erişim Tarihi: 3 Kasım 2016)
- Campbell, K., Gordon, L., Loeb, M., and Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Computer Security, 11, 431–448.
- Canbek, G., ve Sağıroğlu, Ş. (2006). *Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme*. Gazi Üniversitesi Politeknik Dergisi, 9(3), 165-174.
- Carr, N. (2003). *It doesn't matter*. Harvard Business Review 81 (5), 41-49.
- Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. Int. J. Electron. Commerce, 9, 69–104.
- CCDCOE. (2009). *Tallinn manual on the international law applicable to cyber warfare*. Talinn: NATO Cooperative Cyber Defence Centre of Excellence.
- Cherdantseva, Y., and Hilton, J. (2013). *A reference model of information assurance & security. Availability, reliability and security (ARES)*, 2013 Eighth International Conference (pp. 546 - 555). Regensburg: IEEE.
- Chinn, D., Kaplan, J., and Weinberg, A. (2014). Risk and responsibility in a hyper-connected world: implications for enterprises insights and publications. McKinsey & Company.
- Coady, C. (1996). *Terörün ahlakı, cogito (şiddet)*. İstanbul: Yapı Kredi Yayınları, Kış-Bahar.
- COBIT. (24 Ekim 2016). COBIT 5. COBIT 5: <http://www.isaca.org/cobit/pages/default.aspx>_(Erişim Tarihi: 12 Aralık 2016)
- Cridland, C. (2008). The history of the internet: the interwoven domain of enabling technologies and cultural interaction, terrorism (ed.), responses to cyber terrorism NATO Science for Peace and Security. Ankara: IOS Press (Cilt 34).
- Crist, J. (2007). *Web based attacks*. SANS Institute InfoSec Reading Room. GIAC Gold Certification.

- Cropf, R. (2008). American public administration: public service for the 21st century. Pearson Education.

CSA. (27 Ekim 2016). *Cloud controls matrix v3.0.1 (10-6-16 update)*. CSA - Cloud Security Alliance : <https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/>

Czosseck, C., Ottis, R., and Ziolkowski, K. (2012). *4th International Conference on Cyber Conflict*. 4th International Conference on Cyber Conflict . NATO CCD COE Publications.

Dağlı, A. (2015). Örgütsel muhalefet ölçünün Türkçe'ye uyarlanması: geçerlilik ve güvenirlik çalışması. *Elektronik Sosyal Bilimler Dergisi*, 14 (53). 198-218.

Denning, P. (1991). *Computers under attack: intruders, worms, and viruses*. USA: Addison-Wesley Publishing Company.

Desai, D. (2013). *Beyond location: Data security in the 21st century*. Communications of the ACM, 56(1), 34-36. doi:10.1145/2398356.2398368

Dhillon, G., and Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11, 127–153.

DHS. (2016). *Continuous diagnostics and mitigation (CDM)*. ABD İçişleri Bakanlığı: <https://www.dhs.gov/cdm> (Erişim Tarihi: 18 Ekim 2016)

Dimopoulos, V., Furnell, S., Jennex, M.E., and Kritharas, I., *Approaches to IT security in small and medium enterprises*. In Proceedings of the 2nd Australian Information Security Management Conference, Securing the Future, Perth, Australia, 26 November 2004; pp. 73–82.

Dingledine, R., Mathewson, N., and Syverson, P. (2004). *Tor: the second-generation onion router*. SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium, 13, pp. 21-21.

DTIC. (2012). *Objective 3.3 Lexicon & Abbreviations MNE7 Multinational Experiment 7 "Access to the Global Commons"*. Defense Technical Information Center. <http://www.dtic.mil/dtic/tr/fulltext/u2/a590834.pdf> (Erişim Tarihi: 3 Ocak 2017)

EC Council-CEH. (2016). *Certified Ethical Hacker - InfoSec Cyber Security Certification*. International Council of E-Commerce Consultants: <https://www.eccouncil.org/> (Erişim Tarihi: 24 Agustos 2016)

Efe, A. (2006). *Yeni nesil internet Protokoli'ne (IPv6) geçişle birlikte internet saldırularının geleceğine yönelik bekleneler*. Akademik Bilişim 2006, (s. 134 Numaralı Bildiri). Denizli: Akademik Bilişim. <http://ab.org.tr/ab06/bildiri/134.doc> (Erişim Tarihi: 25 Ekim 2016)

- Eminağaoglu, M. (2008). *Dikkat Casus Var! Bilgi Güvenliği Yazı Dizisi*. İstanbul:Tekborsa Dergisi, p. Sayı:15.
- Erbschloe, M. (2005). Trojans, worms, and spyware: a computer security professional's guide to malicious code. . Burlington,MA: Elsevier Butterworth-Heinemann.
- ERIA. (2009). *Strengthening Information Security in the Business Sector (FY2009)*. Jakarta: The Economic Research Institute for ASEAN and East Asia (ERIA). 2016, from http://www.eria.org/publications/research_project_reports/strengthening-information-security-in-the-business-sector-1.html_(Erişim Tarihi: 15 Ocak 2017)
- FFIEC. (2016). *FFIEC Information Technology Examination Handbook*. FFIEC. http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.(Erişim Tarihi: 25 Ekim 2016)
- Filkins, B. (2016). *A Sans Survey. IT Security Spending Trends*. SANS Institute. www.sans.org/reading-room/whitepapers/leadership/security-spending-trends-36697. (Erişim Tarihi: 15 Agustos 2016)
- Fischer, A. E. (2009). Creating a National Framework for Cybersecurity: an Analysis of Issues and Options. New York: Nova Sience Publisher Inc.
- Gady, F.-S. (2016). *Top US Spy Chief: China Still Successful in Cyber Espionage Against US*. The Diplomat: http://thediplomat.com/2016/02/top-us-spy-chief-china-still-successful-in-cyber-espionage-against-us_(Erişim Tarihi: 22 Agustos 2016)
- Gehrman, M. (2012). Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations. *Navus - Revista de Gestão e Tecnologia*, 2(2), 66-77.
- Goel, S., and Chen, V. (2008). Can business process reengineering lead to security vulnerability: analyzing the reengineered process. *International Journal of Production Economics* 115 (1), 104-112.
- Goldman, G. (2011). *Mass e-mail breach: Just how bad is it?* CNN Money http://money.cnn.com/2011/04/06/technology/epsilon_breach/index.htm (Erişim Tarihi: 3 Aralık 2016)
- Gordon, S., and Chess, D. (1999). *Attitude Adjustment: Trojans and Malware on the Internet*. Proceedings of the EICAR Conference. Aalborg, Denmark.
- Gökçen, H. (2002). *Yönetim Bilgi Sistemleri*. Ankara: Epi Yayıncılık.
- Gökçen, H. (2007). *Yönetim Bilgi Sistemleri*. Ankara: Palme Yayıncılık.
- Güngör, M. (2015). *Ulusal Bilgi Güvenliği: Strateji Ve Kurumsal Yapılanma*, Uzmanlık Tezi. Ankara: TC. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı.

- Gürbüz, S. ve Şahin, F. (2016). *Sosyal Bilimlerde Araştırma Yöntemleri: Felsefe-Yöntem-Analiz*, 3. Baskı, Ankara: Seçkin Yayıncılık.
- Gürkaynak, M., ve İren, A. A. (2011). *Reel Dünyada Sanal Açıma: Siber Alanda Uluslararası İlişkiler*. Süleyman Demirel Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi, 16, 263-279.
- Hagen, J. M., Albrechtsen, E., and Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4), 377-397.
- Hanaylı, M. (2014). *Linux Tabanlı Ftp Sunucularda Veri Transferinde Algoritmalar Yardımıyla Güvenli Erişim Yönetimi Uygulaması*. Dumlupınar Üniversitesi, Fen Bilimleri Enstitüsü Matematik Anabilim Dalında Yüksek Lisans Tezi.
- Hansen, L., and Nissenbaum, H. (2009). *Digital Disaster, Cyber Security, and the Copenhagen School*. International Studies Quarterly, 53, 1155-1175.
- Hassinen, T., (2017) *Enhancing Cyber Security for SME organizations through self-assessments How self-assessment raises awareness* Master's Thesis April 2017 School of Technology Master's Degree Programme in Information Technology Cyber Security
- Hemphill, A. T., and Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society*, 44, 30-38.
- Herrmann, D. S. (2007). *Complete Guide To Security and Privacy Metrics Measuring Regulatory Compliance, Operational Resilience, and ROI*. New York: Auerbach Publications.
- Hildreth, S. (2001). *Cyberwarfare Congressional Research Service Report for Congress*. DC: Congressional Research Service & The Library.
- Hoffer, J. A., and Straub, D. W. (1989). *The 9 to 5 underground: Are you policing computer crimes*. Sloan Management Review, 30(4), 35-43.
- Huang, C., Farn, K., and Lin, F., (2011). *A Study on Information Security Management with Personal Data Protection*. 2011 IEEE 17th International Conference on Parallel and Distributed Systems (pp. 624-630). IEEE Computer Society.
- Hutcheson, G. and Sofroniou, N. (1999) *The Multivariate Social Scientist: Introductory Statistics Using Generalized Linear Models*. Sage Publication, Thousand Oaks, CA.
- IAD. (2016). *Manageable Network Plan Guide (version 4.0)*. Information Assurance: <https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/security-configuration/networks/assets/public/upload/manageable-network-plan-guide.pdf&WpKes=aF6woL7fQp3dJiQy4zLnU2u8sNVpdxKAnjUjkp>. (Erişim Tarihi: 25 Ekim 2016)

- Intoccia, G., and Moore, W. J. (2006). *Communications Technology, Warfare, and the Law: Is the Network a Weapon System*. Houston Journal of International Law, 28, 467-489.
- IPA. (2016). *Information Technology Promotion Agency*. IPA: http://www.ipa.go.jp/security/english/benchmark_system.html_(Erişim Tarihi: 20 Ekim 2016)
- Ipsos Mori. (2016). *Cyber Security Breaches Survey 2016 Main Report*. London: Ipsos MORI's Social Research Institute. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf_(Erişim Tarihi: 5 Ekim 2016)
- ISACA. (2015). *CISM Review Manual*, 14th Edition. ISACA.
- ISACA. (2016). *COBIT Global Regulatory and Legislative Recognition*. ISACA: <http://www.isaca.org/COBIT/Pages/Recognition.aspx>_(Erişim Tarihi: 23 Ekim 2016)
- Ismail, R., and Zainab, A. (2011). *Information systems security in special and public libraries: an assessment of status*. Malaysian Journal of Library & Information Science, 16(2), 45-62.
- ISO. (2015). *ISO Survey 2015*. ISO.ORG. <http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO%209001&countrycode=AF>_(Erişim Tarihi: 20 Ekim 2016)
- ISO/IEC 27002. (2016). *ISO/IEC 27002 Information technology -- Security techniques -- Code of practice for information security controls*. ISO.ORG: http://www.iso.org/iso/catalogue_detail?csnumber=54533_(Erişim Tarihi: 25 Ekim 2016)
- ITIL. (2016). *What is ITIL? Best Practice?* Axelos: <https://www.axelos.com/best-practice-solutions/itil/what-is-itil>_(Erişim Tarihi: 27 Ekim 2016)
- ITU. (2015). *ITU Facts and Figures*. ITU Telecommunication Development Bureau. <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>_(Erişim Tarihi: 25 Ekim 2016)
- Jang-Jaccard, J., and Nepal, S. (2014). *A survey of emerging threats in cyber security*. Journal of Computer and System Sciences, 80, 973–993.
- Kalaycı, Ş. (2008). *SPSS uygulamalı çok değişkenli istatistik teknikler*. 3.Baskı, Ankara: Asıl Yayın Dağıtım.
- Kanno, Y. (2005). *Information Security Measures Benchmark (ISM-Benchmark)*. Tokyo: Information-technology Promotion Agency (IPA) Japan. <https://www.ipa.go.jp/files/000011796.pdf>_(Erişim Tarihi: 15 Haziran 2016)

- Kara, M. (2013). *Siber Saldırılar - Siber Savaşlar Ve Etkileri*. İstanbul: Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı.
- Karasar, N. (2008). *Bilimsel Araştırma Yöntemi*. Ankara: Nobel yayın Dağıtım.
- Karri, R., Rosenfeld, K., Rajendran, J., and Tehranipoor, M. (2010). *Trustworthy Hardware: Identifying and Classifying Hardware Trojans*. IEEE Computer, 43, 39-46.
- Karunaratne, J. (2016). *The Passive Splice Network Tap*. Janitha: <http://www.janitha.com/articles/passive-splice-network-tap/> (Erişim Tarihi: 5 Ekim 2016)
- Kauppinen, T., and Kivikoski, J. (2016) *Tutkimus suomalaisen PK-yritysten digitaalisuudesta ja tietoturvasta*. Helsinki. Principal Elisa Oyj and Yrittäjäsanomat. <http://hub.elisa.fi/download/9327/> (Erişim Tarihi: 10 Ekim 2016)
- Keskin, F. (1998). Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler. Ankara: Öteki Matbaası.
- Klimburg, A. (2012). *National Cyber Security Framework Manual*. NATO CCD COE Publications.
- KOSGEB, (2016). *KOBİ Tanımı Değişti*, KOSGEB, http://www.kobi.org.tr/index.php?option=com_content&view=article&id=239:kob-tanm-deiti&itemid=348 (Erişim Tarihi: 17 Mayıs 2016)
- Kong, F., and Li, M. (2013). *Hardware Attacks*. In A. Miri, Advanced Security and Privacy for RFID Technologies (pp. 33-44). Hershey,PA: IGI Global.
- Konrad, A. (2013). Feds Say They've Arrested 'Dread Pirate Roberts,' Shut Down His Black Market' The Silk Road. Forbes 2013,7.
- Krutz, R. L., and Vines, R. D. (2007). *The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*. Indianapolis, IN: Wiley Publising Inc.
- Kudat, B. (2007). Kötü adamların hızına yetişen daha güvenli. BThaber, 6004:15.
- Küçüksille, E. U., Yalçınkaya, M. A., ve Uçar, O. (2014). *Siber Saldırılarda İstismar Kitlerinin Kullanımı Üzerine Bir Analiz ve Savunma Önerileri*. 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı. İstanbul: ISC Turkey.
- Lachow, I. (2013). *Active Cyber Defense A Framework for Policymakers*. Center for a New American Security.
- Li, Q. (2007). Bullying in the new playground: Research into cyberbullying and cyber victimisation. Australasian Journal of Educational Technology, 23(4), 435-454.

- Li, Q., Gao, H., Xu, B., and Jiao, Z. (2008). *Hardware Threat: the Challenge of Information Security*. International Symposium on Computer Science and Computational Technology. IEEE Computer Society.
- Liu, S., and Cheng, B. (2009). *Cyberattacks: Why, What, Who, and How*. IT Professional Magazine, 11(3), 14-21.
- Loeb, L. (2002). *Information Assurance Powwow Part 1*. IEEE Systems, Man, and Cybernetics Information Assurance Workshop. IEEE.<http://www.ibm.com/developerworks/security/library/s-confnotes2/> (Erişim Tarihi: 5 Aralık 2016)
- Malhotra, N. K. (2004) *Marketing research: an applied orientation, 4th edition*, Prentice-Hall International, London.
- Marinos, L., Belmonte, A., and Rekleitis, E. (2016). *ENISA Threat Landscape 2015*. European Union Agency For Network And Information Security.
- Maskun, A., Manuputty, A., Noor, S., and Sumardi, J. (2013). *Cyber Security: Rule of Use Internet Safely*. Socail and Behavioral Sciences 103, 255-261.
- McCumber, J. (1991). *Information systems security: A comprehensive model*. Proceedings 14th National Computer Security Conference. Baltimore: National Institute of Standards and Technology.
- McHugh, J., Christie, A., and Allen, J. (2000). *Defending Yourself: The Role of Intrusion Detection Systems*. IEEE Software, 17(5), 42-51.
- McMaster Üniversitesi. (2016). *IP (Internet Protocol) Spoofing*. McMaster University- Computer and Software Engineering:http://wiki.cas.mcmaster.ca/index.php/IP_Spoofing (Erişim Tarihi: 25 Agustos 2016)
- Meray, S. L. (1962). *Devletler Hukukuna Giriş*. Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları.
- Meydan, C. H. ve Şeşen, H. (2015) *Yapısal Eşitlik Modellemesi AMOS Uygulamaları*, Seçkin Yayınevi, Ankara.
- Mil, H. İ.,(2015) *Sosyal Güvenlik Kurumundaki Siber Güvenlik Yönetimi Uygulamalarının İncelenmesi ve Değerlendirilmesi*, Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Nisan 2015 YIL-7 S.13 sh.398-416.
- Mirdas, A. (2016). *Terör Nedir Ne Dgildir*. Akademik Perspektif: <http://akademikperspektif.com/2013/11/28/teror-nedir-ne-degildir/> (Erişim Tarihi: 26 Agustos 2016)
- Mitnick, K. D., and Simon, W. L. (2003). *The art of deception: controlling the human element of security*. Indianapolis, Indiana: Wiley & Sons.
- NC State University. (2016). *IT Security*. NC State University, Office of Information Technology: <https://oit.ncsu.edu/it-security/safe-computing/spyware/> (Erişim Tarihi: 2 Eylül 2016)

- NCSL. (2016). *Security Breach Notification Laws*. National Conference of State Legislatures: <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>_(Erişim Tarihi: 5 Ekim 2016)
- NERC. (2016). *Critical Infrastructure Protection Standards*. The North American Electric Reliability Corporation: <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx> (Erişim Tarihi: 27 Ekim 2016)
- New Scientist Magazine. (2016). *New Scientist Magazine, Issue 2844 “Dot-dash-diss: The gentleman hacker’s 1903 lulz”*. New Scientist Magazine. Issue 2844: <http://www.newscientist.com/article/mg21228440.700-dotdashdiss-thegentleman-hackers-1903-lulz.html>_(Erişim Tarihi: 10 Temmuz 2016)
- NIST. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. Computer Security Division. Gaithersburg, MD: National Institute of Standards and Technology (NIST). <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf> (Erişim Tarihi: 11 Ekim 2016)
- NIST. (2016). *Cybersecurity Framework*. National Institute of Standards and Technology. <https://www.nist.gov/programs-projects/cybersecurity-framework> (Erişim Tarihi: 25 Agustos 2016)
- Nickolov, E. (2008). Modern trends in the cyber attacks against the critical information infrastructure. Regional Cybersecurity Forum, 7-9.
- Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology*, 2, 61-73.
- Okoye, S.,(2017) *Strategies to Minimize the Effects of Information Security Threats on Business Performance*, College of Management and Technology, Walden University, Doctoral Study 2017
- Ottekin, F. (2016). *Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri*. Bilgi Güvenliği: <https://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenliginde-iso-27000-standartlarinin-yeri-ve-oncelikli-iso-27002-kontrolleri.html>_(Erişim Tarihi: 21 Ekim 2016)
- Öcüt, A. (2016). *Mail ile Gelen TTNET Faturalarına Dikkat Ediniz*. Adem Öcüt Kişisel Blog: <http://ademocut.com/mail-ile-gelen-ttnet-faturalarina-dikkat-ediniz/>(Erişim Tarihi: 10 Aralık 2016)
- Öğüt, A. (2003). *Bilgi Çağında Yönetim* (2. Baskı). Ankara: Nobel Yayın Dağıtım.
- Özdamar, K., Odabaşı, Y., Hoşcan, Y., Kircaali-İftar, G., Özmen, A., ve Uzuner, Y. (1999). *Sosyal Bilimlerde Araştırma Yöntemleri*, (Edt.Ali Atıf Bir). Eskişehir: Anadolu Üniversitesi Açıköğretim Fak.Yay.

- Panko, R. (2009). *Business computer and network security*. Englewood Cliffs, NJ: Prentice-Hall.
- Parker, D. (2010). Our Excessively Simplistic Information Security Model and How to Fix It. *ISSA Journal*, 12-21.
- Patchin, J., and Hinduja, S. (2006). *Bullies move beyond the schoolyard: A preliminary look at cyberbullying*. *Youth Violence and Juvenile Justice*, 4, 148-169.
- PCI SSC. (2016). *Requirements and Security Assessment Procedures*. PCI Security Standards Council: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (Erişim Tarihi: 29 Ekim 2016)
- Persadha, P., Waskita, A., and Yazid, S. (2016). *Comparative Study of Cyber Security Policies among Malaysia, Australia, Indonesia: A Responsibility Perspective*. Proceedings - 4th International Conference on Cyber Security, Cyber Warfare, and Digital Forensics, CyberSec 2015 (pp. 146-150). Jakarta: IEEE.
- Ponemon Institute Research. (2015). *2015 Cost of data breach study: Global Analysis*. Ponemon Institute L.L.C.
- Popular Sience. (1970). Popular Sience Popular Sience <http://www.popsci.com/archive-viewer?id=8QAAAAAAMBAJ&pg=66> (Erişim Tarihi: 3 Ekim 2016)
- Post, J. V. (1979). *Cybernetic War*, The Omni Book of Computers & Robots. Zebra Books.
- PwC. (2016). *The Global State of Information Security Survey 2016*. PwC. Agustos 12, 2016, <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/data-explorer.html>
- Radikal Gazetesi. (2016). *Radikal Ekonomi*. Radikal Gazetesi Web Sitesi: <http://www.radikal.com.tr/haber.php?haberno=240161> (Erişim Tarihi: 28 Eylül 2016)
- Rifat, İ. R., ve Zerenler, M. (2008). *Turizm İşletmelerinde Yönetim Bilişim Sistemleri Kullanımının Yönetsel Kararlar Üzerindeki Etkisi*. S.Ü Sosyal Ve Ekonomik Araştırmalar Dergisi(1(15)), 375-391.
- Richardson, R. (2008). 2008 CSI/FBI Computer Crime & Security Survey. CSI.
- Richardson, R. (2011). *2011 CSI Computer Crime and Security Survey*. Computer Security Institute.
- Richardson, R. (2011). *CSI Computer Crime and Security Survey*. Computer Security Institute.

- Rid, T. (2012). *Cyber War Will Not Take Place*. Journal of Strategic Studies, 35(1).
- Ridley, G., Young, J., and Carroll, P. (2004). *COBIT and its utilization: a framework from the literature*. System Sciences, Proceedings of the 37th Annual Hawaii International Conference (p. 8). IEEE.
- Risk Based Security. (2015). *2015 Reported Data Breaches Surpasses All Previous Years*. Risk Based Security. <https://www.riskbasedsecurity.com/2016/02/2015-reported-data-breaches-surpasses-all-previous-years/> (Erişim Tarihi: 13 Kasım 2016)
- Rogin, J. (2012). *NSA Chief: Cybercrime constitutes the “greatest transfer of wealth in history”*. Foreign Policy: <http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/> (Erişim Tarihi: 9 Kasım 2016)
- Salem, M. B., Shlomo, H. S., and Stolfo, S. J. (2008). *A Survey of Insider Attack Detection Research*. Insider Attack and Cyber Security, 39, 69-90.
- Saltzer, J., and Schroeder, M. (1975). *The protection of information in computer systems*. Proceedings of the IEEE. 63(9), pp. 1278-1308. IEEE.
- Schmid, A. P. (1993). The Response Problem As a Definition Problem, Western Responses to Terrorism. England: Frank Cass & Co. Ltd.
- Schneier, B. (2008). *Schneier on Security*. USA: John Wiley & Sons Inc.
- Scott. (2016). *Why HTTPS and SSL are not as secure as you think*. Scott.Net: <https://www.scott.net/article/275524-Why-HHTPS-and-SSL-are-not-as-secure-as-you-think> (Erişim Tarihi: 13 Ekim 2016)
- Segev, A., Porra, J., and Roldan, M. (1998). *Internet security and the case of Bank of America*. Communications of the ACM, 41, 81-87.
- Shahriar, H., and Zulkernine, M. (2012). Mitigating program security vulnerabilities: Approaches and challenges, ACM Computer Survey., 44(3).
- Sisaneci, İ., Akin, O., Karaman, M., and Saglam, M. (2013). *A Novel Concept For Cybersecurity: Institutional Cybersecurity*. 6th International Conference on Information Security and Cryptology, 89.
- Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? Computers and Security, 24, 99-104.
- Solms, V., and Niekerk, V. (2013). *From Information security to Cyber Security*. Computers & Security 38, 97-102.
- Srikantaswamy, S., and Phaneendra, H. (2012). *Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption*. International Journal on Cryptography and Information Security (IJCIS), 2(4), 39-49.

- SSL Shop. (2016). *Eavesdropping Attack: A Dark Shadow on the Network*. SSL Shop: <https://www.cheapsslshop.com/blog/eavesdropping-attack-a-dark-shadow-on-the-network>_(Erişim Tarihi: 25 Ağustos 2016)
- Stallings, W. (2006). Cryptography and network security: principles and practices. Pearson Education.
- Stop-Think-Connect. (2016). *Back Up Poster*. Stop-Think-Connect: https://www.stopthinkconnect.org/resources/preview/back-up-poster_(Erişim Tarihi: 19 Ekim 2016)
- Straub, D., and Welke, R. (1998). Coping with systems risks: security planning models for management decision making. *MIS Quarterly*, 22, 441–469.
- Sundt, C. (2006). *Information security and the law*. Information Security Technical Report, 11(1), 2-9.
- Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., ve Borandağ, E., *Kurumlarda Bilgi Güvenliği Farkındalıkı, Önemi ve Oluşturma Yöntemleri*, Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri 11-13 Şubat 2009 sh.597-602 Harran Üniversitesi, Şanlıurfa
- Şentürk, H., Çil, C. Z., and Sağıroğlu, Ş. (2012). *Cyber Security Analysis of Turkey*. International Journal of Information Security Science, 1(4), 112-125.
- T.C Ulaştırma Bakanlığı. (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi*. Ankara: T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı.
- Tarcan, M., Gul, Y., Gul, F., and Tarcan, G. (2010). The Exchange Ratio In The Dimensions Of Integrity, Confidentiality And Availability Of Information Security In The Teaching And General Hospitals: Case Study Of Ministry Of Health Hospitals Of Turkey. Northeast Decision Sciences Institute Proceedings, (p. 610).
- Tekin, M., Güles, H., ve T., B. (2000). *Dünyadaki Teknoloji Yönetimi Bilişim Teknolojileri*. Konya: Damla Ofset.
- Thomson, K. L., and Solms, R. V. (2005). *Information security obedience:a definition*. Computers & Security, 24, 69-75.
- Tipton, H., and Krause, M. (2007). *Information Security Management Handbook*. Auerbach Publicaions.
- Tomlin M., (2015) *Advancing Small Business Cyber Maturity: An application of the NIST Cybersecurity Framework*. Master's thesis, Royal Holloway, University of London, 2015.
- TS ISO/IEC 27001:2013. (2016). Bilgi Güvenliği Yönetim Sistemi Standardı.

- Tsukayama, H. (2011) *Cyber attack was large-scale, Sony says*. Washington Post https://www.washingtonpost.com/blogs/faster-forward/post/cyber-attack-waslarge-scale-sony-says/2011/05/04/AF78yDpF_blog.html (Erişim Tarihi: 25 Ocak 2017)
- Türk Ansiklopedisi. (1958). *Türk Ansiklopedisi, Cilt 9*. Ankara: Maarif Basımevi.
- Türk Dil Kurumu. (2017). *Güncel Türkçe Sözlük* http://www.tdk.gov.tr/index.php?option=com_gts&view=gts (Erişim Tarihi: 17 Mayıs 2016)
- UDHB (2016). *Siber Güvenlik*. Ulaştırma Denizcilik ve Haberleşme Bakanlığı: <http://www.udhb.gov.tr/h-12-siberguvenlik.html> (Erişim Tarihi: 27 Ekim 2016)
- UK Cyber Essentials. (2014). *Cyber Essentials Scheme*. GOV.UK. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf (Erişim Tarihi: 18 Ekim 2016)
- UK ICO. (2016). *Data protection self assessment toolkit*. ICO: <https://ico.org.uk/for-organisations/improve-your-practices/data-protection-self-assessment-toolkit/> (Erişim Tarihi: 15 Eylül 2016)
- UK-NCSC. (2016). *10 Steps: Summary*. UK National Cyber Security Centre: https://www.ncsc.gov.uk/guidance/10-steps-executive-summary_ (Erişim Tarihi: 5 Eylül 2016)
- Ünver, M., Canbay, C., ve Mirzaoğlu, A. (2011). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*. Ankara: Bilgi Teknolojileri ve İletişim Kurumu.
- Vacca, R. J. (2006). *Guide to Wireless Network Security*. Pomeroy, OH: Springer Science & Business Media LLC.
- Valenzuela, I. (2016). *Game Changer: Identifying and Defending Against Data Exfiltration Attempts*. SANS Cyber Defense Summit. Nashville, TN: SANS. https://files.sans.org/summit/Cyber_Defense_Summit_2015/PDFs/Identifying-and-Defending-Against-Data-Exfiltration-Attempts-Ismael-Valenzuela-Foundstone.pdf (Erişim Tarihi: 3 Eylül 2016)
- Valli, C., Martinus, I., ve Johnstone, M. (2014). *Small to medium enterprise cyber security awareness: An initial survey of Western Australian business*. In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). <http://worldcomp-proceedings.com/proc/p2014/SAM9779.pdf> (Erişim Tarihi: 10 Ağustos 2016)

- Vardal, N. (2009). *Yükseköğretimde Bilgi Güvenliği: Bilgi Güvenlik Yönetim Sistemi İçin Bir Model Önerisi Ve Uygulaması.* (Yayınlanmış doktora tezi). Ankara: Gazi Üniversitesi/Eğitim Bilimleri Enstitüsü.
- Verizon. (2016). *Verizon's 2016 Data Breach Investigations Report.* Verizon. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf (Erişim Tarihi: 2 Aralık 2016)
- Von Solms, B. (2000). *Information security – the third wave?* Computers & Security, 19(7), 615-620.
- Vorakulpipat, C., Siwamogsatham, S., and Pibulyarojana, K. (2010). *Exploring Information Security Practices in Thailand Using ISM-Benchmark.* Technology Management for Global Economic Growth (PICMET), 2010 Proceedings of PICMET '10 (pp. 1-4). Phuket: IEEE.
- Vural, Y. ve Sağiroğlu, Ş. (2011). *Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler,* Gazi Univ. Müh. Mim. Fak. Der. Cilt 26, No 1, 89-103, 2011
- Vural, Y., ve Sağiroğlu, Ş. (2008). *Kurumsal Bilgi Güvenliği ve Standartları Üzrine bir inceleme.* Gazi Üniversitesi Müh. Mimarlık Fakültesi Dergisi Cilt 23, No 2, 507-522.
- Ware, H. (1979). *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security - RAND Report R-609-1.* Santa Monica: The Rand Corporation. <http://www.rand.org/pubs/reports/R609-1/index2.html> (Erişim Tarihi: 15 Ekim 2016)
- Wei, O. K. (2016). *Reality: Security and Spending Are Unbalanced.* IBM Software Group: http://www-07.ibm.com/sg/smarterbusiness/meettheexperts/includes/downloads/Securing_Your_Web_0910_eve.pdf. (Erişim Tarihi: 29 Ekim 2016)
- Weimann, G. (2006). *Terror On The Internet: The New Arena The New Challenges,* . Washington D.C.: United States Institutue Of Peace.
- Whitman, M. (2003). *Enemy at the gate: threats to information security.* Communications of the ACM, 46(8), 91-95.
- Whitman, M., and Mattord, H. (2012). *Principles of Information Security, 4th ed.* Cengage Learning.
- Winther, R., Gran, B. A., and Dahll, G. (2005). *Computer Safety, Reliability, and Security.* 24th International Conference SAFECOMP 2005, (p. 371). Fredrikstad, Norway.
- Wolf, J., and Maclean, W. (2011). IMF cyber attack aimed to steal insider information: Expert. Reuters <http://www.reuters.com/article/2011/06/12/us-imfcyberattack-idUSTRE75A20720110612> (Erişim Tarihi: 19 Kasım 2016)

- Wood, C. C. (2005). *Information Security Policies Made Easy*. Houston,TX: Information Shield.
- Yaşar, H., ve Çakır, H. (2015). *Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri*. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3, 488-507.
- Yavanoğlu, U., Sağıroğlu, Ş., ve Çolak, İ., *Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler*, Politeknik Dergisi, Cilt:15 Sayı: 1 s. 15-27, 2012.
- Yayla, A., and Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, 26, 60-77.
- Yazıcıoğlu, Y. ve Erdoğan, S. (2004). *SPSS Uygulamalı Bilimsel Araştırma Yöntemleri*. Ankara: Detay Yayıncılık.
- Yeh, Q.J., and Chang, A. J. (2007). Threats and Countermeasures for Information System Security: A Cross-Industry Study. *Information & Management*, 44(5), 480-491.
- Yeşilyurt, H.(2015) *Finansal Hizmet Sektöründe Siber Güvenlik Riskleri Ve Çözüm Yolları: Ödeme Sistemleri ve Tedarik Zinciri Büyünlüğü*, CBÜ Sosyal Bilimler Dergisi, Cilt:13, Sayı:2, Haziran 2015 sh.97-120.
- Yılmaz, E., Ulus, H.İ., ve Gönen, S., *Bilgi Toplumuna Geçiş ve Siber Güvenlik*, Bilişim Teknolojileri Dergisi, Cilt: 8, Sayı: 3, Eylül 2015 s. 133-146.
- Zhang, H., Han, W., Lai, X., Lin, D., Ma, J., and Li, J. (2015). *Survey on cyberspace security*. *Science China, Information Sciences*, 58, 110101:1–110101:43.
- Zikmund, W. G. (2002). *Business Research Methods*. Nashville, TN: South-Western College Pub.